MSP7-32-256-4XC MACsec Core

5-12.5G, 32 bit interface for FPGA or ASIC

General Description

Implementation of the LAN security standard IEEE 802.1ae (MACsec) requires the NIST standard AES cipher in the GCM mode for encryption and message authentication, as well as header parsing and formatting operations on the transmitted and received packets. MACsec Security Processor (MSP) IP cores by IP Cores, Inc. are designed for high data rates and implement complete line-rate packet processing with no per-packet CPU intervention. The MSP7-32 cores are tuned for 6-15 Gbps applications in the FPGA and ASIC technologies that require 256 bit AES keys.

The design is fully synchronous and available as RTL source code.

Key Features

Small size combined with high performance:

- 5 Gbps performance at the 156+ MHz clock rate
- 12.5 Gbps performance at the 390+ MHz clock rate

Flow-through design with back-to-back packet processing

- 41-byte-long shortest input packet on encryption[1]
- 56-byte-long shortest input packet on decryption at full data rate[2]
- 16,000 bytes maximum packet size

Low latency, for the 10 Gbps configuration:

- 34 clocks input-to-output on encryption (start-to-start of the packet), 36-37 clocks (last-to-last word of the packet);
- 39 clocks for decryption (start-to-start), 37 clocks (last to last).

[1] Shorter frames are passed through at full rate but cannot be processed and are marked as **invalid_packet**.

[2] Shorter frames are passed through at full rate but cannot be processed and are marked as **invalid_packet**.

32-bit wide aligned[3] AXI-S data interface with flow control.

- The MSP7 contains two datapaths, one for Tx (egress, Encryption, E), one for Rx (ingress, Decryption, D). The Tx datapath presents a sink (slave) interface to the unencrypted side, source (master) interface on the encrypted side. Rx datapath presents a sink to the encrypted, source to the unencrypted side.

- Core utilizes three clocks: one for the Tx (egress) datapath, one for Rx (ingress) and one for control

Configuration

The core is designed for 4 Secure Channels (SC)[4], 4 Secure Associations (SAs) per SC.

Support for the 256 bit AES key per IEEE 802.1Aebn standard.

Support for Extended Packet Numbering per IEEE 802.1Aebw (GCM-AES-XPN-128, GCM-AES-XPN-256).

Support for IEEE 802.1Aecg Draft Amendment 3 (Ethernet Data Encryption devices).

Support for the VLAN tags in the clear: move or copy the C-Tag and S-Tag in the header.

Bypass for the PTP data.

AXI4-Lite interface for control.

Provides MACsec header parsing and modification:

- Insertion and removal of the SecTag including the packet number (PN) and an optional SCI
- RX packet validation
- Insertion, validation and removal of the ICV
- Replay protection based on the PN windowing

Includes key storage and expansion.

Support for Galois Counter Mode Encryption and authentication (GCM-AES-128, GCM-AES-256), Galois Message Authentication (GMAC)

External statistics/interrupts block with glueless interface to the core.

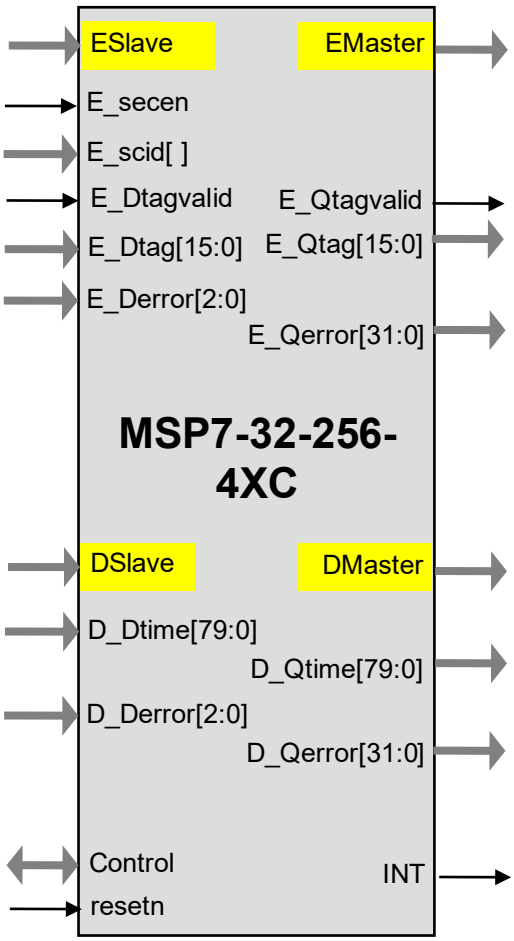
Test bench provided.

Sample SDK for core control and 802.1X implementation.

[3] A new data frame shall always start at the MSB of the data bus
[4] Multiple classification options available covering the range from few SCs to few thousand SCs. This configuration uses external pins for classification on egress, SCI for classification on ingress.

Deliverables include test benches and optional NIST algorithm validation.

Symbol



Pin Description

Name	Type	Description
Generic		
INT	Output	Interrupt signal. See the interrupt descriptions below.
Resetn	Input	Core reset signal, active LOW. This is the global reset shared by all interfaces.
Eclk	Input	Encryption (Tx) datapath clock
Dclk	Input	Decryption (Rx) datapath clock
Eslave Interface is an AXI-S interface with continuous aligned stream.		
Emaster Interface is an AXI-S interface with continuous aligned stream.		
Dslave Interface is an AXI-S interface with continuous aligned stream.		
Dmaster Interface is an AXI-S interface with continuous aligned stream.		
MACsec out of band signaling for encryption (Tx) interface. Prefixed with E_.		
E_Derror[2:0]	Input	Error signal.
E_Qerror[31:0]	Output	Error signal.
E_secen	Input	Enable encryption for this packet.
E_scid[ ]	Input	Secure channel selection for the packet.
E_Dtagvalid	Input	PTP tag
E_Dtag[15:0]	Input	PTP tag.
E_Qtagvalid	Output	PTP tag
E_Qtag[15:0]	Output	Bypassed PTP tag.
MACsec out of band signaling for decryption (Rx) interface. Prefixed with D_.		
D_Derror[2:0]	Input	Error signal.
D_Qerror[31:0]	Output	Error signal.
D_Dtime[79:0]	Input	PTP time stamp
D_Qtime[79:0]	Output	Bypassed PTP time stamp.
CPU interface is either AXI4-Lite, AHB, or APB		

Function Description

The MSP7 implementation fully supports the IEEE 802.1ae (MACsec) algorithm for 256-bit bit keys (IEEE 802.1Aebn), including AES support in Galois Counter Mode (GCM) per NIST publication SP800-38D

http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf and extended packet number per IEEE 802.1Aebw.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Vectors for testbench
- Expected results
- User Documentation

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com